

Maximal prime homomorphic images of mod- p Iwasawa algebras

Billy Woods

August 30, 2016

Abstract

Let k be a finite field of characteristic p , and G a compact p -adic analytic group. Write kG for the completed group ring of G over k . In this paper, we describe the structure of the ring kG/P , where P is a minimal prime ideal of kG . We give an isomorphism between kG/P and a matrix ring with coefficients in the ring $(k'G')_\alpha$, where k'/k is a finite field extension, G' is a large subquotient of G with no finite normal subgroups, and $(-)_\alpha$ is a "twisting" operation that preserves several desirable properties of the ring structure. We demonstrate an application of this isomorphism by setting up correspondences between certain ideals and subrings of kG and those of $(k'G')_\alpha$, and showing that these correspondences often preserve some useful properties, such as almost-faithfulness of an ideal, or control of an ideal by a closed normal subgroup.

Contents

1	Preliminaries	6
2	The untwisting theorem	10
3	Almost faithful ideals	14
4	Untwisting when G is finite-by-(pro- p)	17
5	Central twists by 2-cocycles	21
6	Peirce decomposition	30

Introduction

Let G be a compact p -adic analytic group, and k a finite field of characteristic p . Write kG for the completed group ring of G over k ,

$$kG := \varprojlim_N k[G/N],$$

where the inverse limit ranges over all open normal subgroups N of G , and $k[G/N]$ denotes the ordinary group algebra of the (finite) group G/N over k .

In this paper, we explore the structure of the ring kG/M , where M is an arbitrary minimal prime ideal of kG . It is known already, due to Ardakov [2], that the minimal primes of kG are intimately connected with the minimal primes of $k\Delta^+$, where

$$\Delta^+ = \{x \in G \mid o(x) < \infty, [G : \mathbf{C}_G(x)] < \infty\}$$

is the *finite radical* of G . We review this connection in Lemma 1.1.

Our first result is:

Theorem A. Let H be a compact p -adic analytic group with H/Δ^+ pro- p , and let k be a finite field of characteristic p . Take a minimal prime \mathfrak{p} of $k\Delta^+$ which is H -invariant, so that $\mathfrak{p}kH$ is a minimal prime of kH . Then there exist a positive integer t , a finite field extension k'/k , and an isomorphism

$$\psi : kH/\mathfrak{p}kH \rightarrow M_t\left(k'[[H/\Delta^+]]\right).$$

This is a strengthening of the results in [3, Propositions 10.1, 10.4] and [2], which deal only with simple cases such as the case when $H = F \times U$, for F a finite group and U a uniform pro- p group.

In the proof of this theorem, as elsewhere in this paper, we give a reasonably explicit construction of such an isomorphism, so as to be able to keep track of images of ideals and subrings.

In general, if G is a compact p -adic analytic group, G will have an open normal subgroup H satisfying the conditions of Theorem A; but this may not in general extend to an isomorphism

$$kG/\mathfrak{p}kG \rightarrow M_t\left(k'[[G/\Delta^+]]\right).$$

However, this is not too far off. We show that a similar result does hold, provided we are willing to replace $k'[[G/\Delta^+]]$ by a closely related ring $(k'[[G/\Delta^+]])_\alpha$, a *central 2-cocycle twist* of $k'[[G/\Delta^+]]$. We define this fully in Definition 5.4, and then show that the twisting process $(-)_\alpha$ preserves some desirable properties.

Theorem B. Let G be a compact p -adic analytic group and H an open normal subgroup containing Δ^+ with H/Δ^+ pro- p , and let k be a finite field of characteristic p . Take a minimal prime \mathfrak{p} of $k\Delta^+$ which is G -invariant (note that then

$\mathfrak{p}kH$ is a minimal prime of kH and $\mathfrak{p}kG$ is a minimal prime of kG). Then the isomorphism ψ of Theorem A extends to an isomorphism

$$\tilde{\psi} : kG/\mathfrak{p}kG \rightarrow M_t\left((k'[[G/\Delta^+]])_\alpha\right).$$

Studying this isomorphism in detail allows us to understand the behaviour of ideals of kG containing $\mathfrak{p}kG$ by understanding ideals of $(k'[[G/\Delta^+]])_\alpha$. We derive some consequences of Theorem B that will be useful in later work.

In Definition 1.4 below, we will say that an ideal I of kG is *faithful* if the natural map $G \rightarrow (kG/I)^\times$ is an injection, and *almost faithful* if its kernel is finite. A measure of the failure of I to be faithful is given by the normal subgroup $I^\dagger := \ker(G \rightarrow (kG/I)^\times)$.

Theorem C. With notation as in Theorem B, let A be an ideal of kH containing $\mathfrak{p}kH$. Write $\psi(A/\mathfrak{p}kH) = M_t(\mathfrak{a})$ for some ideal \mathfrak{a} of $k'[[H/\Delta^+]]$. Then

- (i) A is prime in kH if and only if \mathfrak{a} is prime in $k'[[H/\Delta^+]]$.
- (ii) A is stable under conjugation by G if and only if \mathfrak{a} is stable under conjugation by G/Δ^+ in the ring $(k'[[G/\Delta^+]])_\alpha$.
- (iii) A is almost faithful as an ideal of kH if and only if \mathfrak{a} is (almost) faithful as an ideal of $k'[[H/\Delta^+]]$.

We state all of these results together here for convenience. Statement (i) above is an easy consequence of Morita equivalence, given in Lemma 1.7, but statements (ii) and (iii) rely crucially on explicit calculations under the isomorphism ψ .

In the general case, \mathfrak{p} will not necessarily be G -invariant, but may have a (finite) G -orbit, say of size r . In this case, we have:

Theorem D. Let Q be a minimal prime ideal of kG , and let \mathfrak{p} be a minimal prime ideal of $k\Delta^+$ containing $Q \cap k\Delta^+$. Then there is an isomorphism

$$kG/Q \rightarrow M_{rt}\left((k'[[G_1/\Delta^+]])_\alpha\right),$$

where G_1 is the open subgroup of G stabilising \mathfrak{p} .

We prove a much more precise statement of this theorem in section 6, but do not state it here as the notation is rather technical. The more precise statement helps in understanding the relationship between ideals of kG and ideals of kH , when H is a closed normal subgroup of G . When H acts transitively on the G -orbit of \mathfrak{p} , as in the special case of Theorem B, it is not hard to generalise Theorem C; but the G -orbit of \mathfrak{p} may split into several H -orbits, possibly of different sizes, and it is important to keep track of the isomorphism.

As an application of this, we finally prove the following result:

Theorem E. Let P be an ideal of kG , and suppose that $P \cap k\Delta^+$ is contained in each of the minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of $k\Delta^+$, which are all transitively

permuted by G under conjugation. Let H be any closed normal subgroup of G containing Δ^+ . For each $1 \leq i \leq n$, let G_i be the (open) stabiliser in G of \mathfrak{p}_i , and note that G_i must contain Δ^+ . Then we can find an ideal Q_i of $k'G_i$ for each $1 \leq i \leq n$ such that the following properties hold:

- (i) each $Q_i \cap k\Delta^+$ is contained only in the minimal prime ideal \mathfrak{p}_i of $k\Delta^+$;
- (ii) P is controlled by H if and only if each Q_i is controlled by $H \cap G_i$; and
- (iii) $P^\dagger = \bigcap_{i=1}^n Q_i^\dagger$.

1 Preliminaries

Recall the *FC-centre* $\Delta(G)$ and the *finite radical* $\Delta^+(G)$ from [12, Definition 1.2]. We will often write $\Delta = \Delta(G)$ and $\Delta^+ = \Delta^+(G)$ as shorthand throughout this paper.

We record here, for ease of reference, some facts and notation that we will use throughout this paper.

Lemma 1.1. Let G be a compact p -adic analytic group, and k a finite field of characteristic p .

- (i) Write $J := J(k\Delta^+)$. Then JkG is a two-sided ideal of kG contained in the prime radical of kG . Hence, denoting by $\overline{(\cdot)}$ images under the natural map $kG \rightarrow kG/JkG$, there is a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{minimal prime} \\ \text{ideals of } kG \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{minimal prime} \\ \text{ideals of } \overline{kG} \end{array} \right\}.$$

- (ii) Retain the notation of (i).

Let $X = \{e_1, \dots, e_r\}$ be a G -orbit of centrally primitive idempotents of $\overline{k\Delta^+}$, and write $f = e_1 + \dots + e_r$. Then $\overline{M_X} := (1 - f)\overline{kG}$ is a minimal prime ideal of \overline{kG} , hence (by (i)) its preimage M_X in kG is a minimal prime ideal in kG .

Conversely, let M be a minimal prime ideal of kG . Then there exists a G -orbit X of centrally primitive idempotents of $\overline{k\Delta^+}$ such that $M = M_X$.

This sets up a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{minimal prime} \\ \text{ideals of } kG \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} G\text{-orbits of centrally} \\ \text{primitive idempotents of } \overline{k\Delta^+} \end{array} \right\}.$$

- (iii) Given a centrally primitive idempotent $e \in \overline{k\Delta^+}$, there exists some $t > 0$ and some finite field extension k'/k with $e \cdot \overline{k\Delta^+} \cong M_t(k')$. Hence, if A is a k -algebra, we may identify the rings

$$e \cdot \overline{k\Delta^+} \otimes_k A \xrightarrow{\cong} e \cdot \overline{k\Delta^+} \otimes_{k'} (k' \otimes_k A) \xrightarrow{\cong} M_t(k' \otimes_k A).$$

Proof.

- (i) This follows from [2, 5.2].
- (ii) This follows from [2, §5, in particular 5.7].
- (iii) $e \cdot \overline{k\Delta^+}$ is a simple finite-dimensional k -algebra, so the isomorphism $e \cdot \overline{k\Delta^+} \cong M_t(k')$ follows from Wedderburn's theorem. The rest is a simple calculation. \square

We will use this correspondence very often, so will immediately set up notation which we will use for the rest of this paper.

Notation 1.2. If an ideal $I \triangleleft kG$ contains a minimal prime ideal, then it contains a *unique* minimal prime ideal, say M . Then, under the correspondence of Lemma 1.1(ii), we obtain a unique G -orbit X of centrally primitive idempotents of $\overline{k\Delta^+}$ corresponding to M .

Throughout this paper, we will write

$$\text{cpi}^{\overline{k\Delta^+}}(I) \quad (\text{or } \text{cpi}^{\overline{k\Delta^+}}(M))$$

for this set X . Given a centrally primitive idempotent $e \in \text{cpi}^{\overline{k\Delta^+}}(I)$, we will write $f = e|_G$ to mean

$$f = \sum_{g \in \mathbf{C}_G(e) \backslash G} e^g,$$

where $\mathbf{C}_G(e) \backslash G$ denotes the (finite) set of right cosets of $\mathbf{C}_G(e)$ in G . In other words, if we write $e = e_1$ and $X = \{e_1, \dots, e_r\}$, then $f = e|_G$ means $f = e_1 + \dots + e_r$.

In this context, $\overline{(\cdot)}$ will always mean the quotient by JkG unless otherwise stated. Thus,

- $\overline{M} = (1 - f)\overline{kG}$,
- $f \cdot \overline{kG} = \overline{kG}/\overline{M} \cong kG/M$,
- $f \cdot \overline{I} = \overline{I}/\overline{M} \cong I/M$, etc.

Definition 1.3. Let P be a prime ideal of the ring R . We say that P is *controlled by* the subring S if $(P \cap S)R = P$. Following Roseblade [10, 1.1], if $R = kG$ and $S = kH$ for some closed normal subgroup H of G , we say P is *controlled by* H .

Definition 1.4. For any ideal I of kG , define also

$$I^\dagger = \{x \in G \mid x - 1 \in I\}.$$

This is the kernel of the natural group homomorphism $G \rightarrow (kG/I)^\times$, and so is a normal subgroup of G . If $I^\dagger = 1$, we say that I is a *faithful* ideal; if I^\dagger is finite, we say that I is *almost faithful*.

In future work, we will use the techniques in this paper to show that, if G is a nilpotent-by-finite, *orbitally sound* [12, Definition 1.4] compact p -adic analytic group, k is a finite field of characteristic p , and P is a prime ideal of kG with $P^\dagger = 1$, then P is controlled by the subgroup $\Delta(G)$.

The next two lemmas are technical results about controller subgroups: see the remarks at the start of section 3 for the big picture.

Lemma 1.5. Let P be an ideal of kG containing a prime ideal, and write $e = \text{cpi}^{\overline{k\Delta^+}}(P)$, $f = e|_G$ as in Notation 1.2. Let H be any closed subgroup of G containing Δ^+ . Then the following are equivalent:

- $(P \cap kH)kG = P$,
- $(\overline{P \cap kH})\overline{kG} = \overline{P}$,
- $(f \cdot \overline{P \cap kH})f \cdot \overline{kG} = f \cdot \overline{P}$.

Proof. Firstly, $JkG \subseteq P$ by Lemma 1.1(i), and so by the modular law we have

$$(P \cap kH) + JkG = P \cap (kH + JkG)$$

from which we can deduce

$$\overline{P \cap kH} = \overline{P \cap kH},$$

and so

$$\overline{(P \cap kH)kG} = (\overline{P \cap kH})\overline{kG}.$$

Conversely, the preimage in kG of $(\overline{P \cap kH})\overline{kG}$ is $(P \cap kH)kG + JkG$, but this is just $(P \cap kH)kG$ as $J \subseteq P \cap kH$.

Secondly, $(1 - f)\overline{kG} \subseteq \overline{P}$, and so just as above we may deduce by the modular law

$$f \cdot ((\overline{P \cap kH})\overline{kG}) = (f \cdot \overline{P \cap kH})f \cdot \overline{kG}.$$

Similarly, $1 - f \in \overline{P \cap kH}$, so the preimage in \overline{kG} of $(f \cdot \overline{P \cap kH})f \cdot \overline{kG}$ is $(\overline{P \cap kH})\overline{kG}$. \square

In order to retrieve information from Lemma 1.1(iii), we need a matrix control lemma:

Lemma 1.6. Let R be a ring, I an ideal of R , and S a subring of R . Let t be a positive integer. Then the following are equivalent:

- (i) $(I \cap S)R = I$
- (ii) $(M_t(I) \cap M_t(S))M_t(R) = M_t(I)$

Proof.

(i) \Rightarrow (ii) Identify R , S and I with their images under the diagonal embedding $R \hookrightarrow M_t(R)$. It is clear that

$$I \cdot M_t(R) \subseteq M_t(I),$$

and conversely if $a_{kl} \in I$ for all $1 \leq k, l \leq t$ then

$$(a_{ij})_{i,j} = \sum_{k,l} a_{kl} E_{kl}$$

where $E_{kl} \in M_t(R)$ is the elementary matrix with (i, j) -entry $\delta_{ik}\delta_{jl}$. So we see that $I \cdot M_t(R) = M_t(I)$. But clearly

$$\begin{aligned} M_t(I) &= I \cdot M_t(R) = (I \cap S)R \cdot M_t(R) \\ &= (I \cap S)M_t(R) \\ &\subseteq (M_t(I) \cap M_t(S))M_t(R) \\ &\subseteq M_t(I), \end{aligned}$$

and so these are all equal.

(ii) \Rightarrow (i) Intersect both sides of the equation $(M_t(I) \cap M_t(S))M_t(R) = M_t(I)$ with the diagonal copy of R inside $M_t(R)$. \square

Finally, we recall some basic properties of Morita equivalence:

Lemma 1.7. If R and S are Morita equivalent rings, then there is an order-preserving one-to-one correspondence between the ideals of R and the ideals of S , and this correspondence preserves primality. R is Morita equivalent to $M_t(R)$ for any positive integer t .

Proof. This is [7, 3.5.5, 3.5.9]. \square

2 The untwisting theorem

Definition 2.1. [4, Introduction] Let G be a profinite group and k a commutative pseudocompact ring. Then the completed group ring kG is defined to be

$$kG = \varprojlim_N k[G/N],$$

where the inverse limit ranges over all open normal subgroups N of G , and $k[G/N]$ denotes the ordinary group algebra of the (finite) group G/N over k .

Remark. When it helps to reduce ambiguity, we will write kG as $k[[G]]$.

Recall from [7, 1.5.2] that, for any finite group F , there is a natural embedding of groups $i_F : F \rightarrow (kF)^\times$. By taking the inverse limit of the maps $\{i_{G/N}\}$, we get a continuous embedding $i : G \rightarrow (kG)^\times$.

Lemma 2.2 (Universal property of completed group rings). Let G be a profinite group and k a commutative pseudocompact ring. Then the completed group ring kG satisfies the following universal property: given any pseudocompact k -algebra R and any continuous group homomorphism $f : G \rightarrow R^\times$, there is a unique homomorphism $f^* : kG \rightarrow R$ of pseudocompact k -algebras satisfying $f^* \circ i = f$. (Here, $(kG)^\times$ and R^\times are naturally viewed as subsets of kG and R respectively.)

Proof. Let $f : G \rightarrow R^\times$ be a continuous group homomorphism, and let I be an open ideal of R which is a neighbourhood of zero. Then $(I + 1) \cap R^\times$ must be open in R^\times , and so its preimage $I^\dagger := f^{-1}((I + 1) \cap R)$ must be open in G . Thus the map f descends to a homomorphism of (abstract) groups $f_I : G/I^\dagger \rightarrow R^\times/(I + 1) \cap R^\times \rightarrow (R/I)^\times$, and G/I^\dagger is finite.

Now, by the universal property for (ordinary) group rings [7, 1.5.2], we get a ring homomorphism $k[G/I^\dagger] \rightarrow R/I$ extending f_I , and hence a ring homomorphism $kG \rightarrow k[G/I^\dagger] \rightarrow R/I$ by definition. But as R is the inverse limit of these R/I , we get a continuous ring homomorphism $kG \rightarrow R$ extending f . \square

Definition 2.3. [4, §2] Let k be a commutative pseudocompact ring and R a pseudocompact k -algebra. Let A be a right and B a left pseudocompact R -module: then the *completed tensor product* $A \hat{\otimes}_R B$ is a k -module defined by

$$A \hat{\otimes}_R B = \varprojlim_{U,V} (A/U \otimes_R B/V),$$

where U and V range over the open submodules of A and B respectively.

Definition 2.4 (Universal property of completed tensor product). [4, §2] Let R be a pseudocompact k -algebra, and let A be a right and B a left pseudocompact R -module. Then the completed tensor product

$$A \hat{\otimes}_R B$$

is a k -module satisfying the following universal property: there is a unique R -bihomomorphism

$$A \times B \rightarrow A \hat{\otimes}_R B$$

through which any given R -bihomomorphism $A \times B \rightarrow C$ into a pseudocompact k -module C factors uniquely. (An R -bihomomorphism $\theta : A \times B \rightarrow C$ is a continuous k -module homomorphism satisfying $\theta(ar, b) = \theta(a, rb)$ for all $a \in A, b \in B, r \in R$.)

If $R = k$, and A and B are k -algebras, then their completed tensor product is also a k -algebra.

Theorem 2.5 (untwisting). Let G be a compact p -adic analytic group, k a commutative pseudocompact ring, and kG the associated completed group ring. Suppose H is a closed normal subgroup of G , and I is an ideal of kH such that $I \cdot kG = kG \cdot I$. Write $\overline{(-)} : kG \rightarrow kG/IkG$, so that $\overline{kH} = kH/I$. Suppose also that we have a continuous group homomorphism $\delta : G \rightarrow \overline{kH}^\times$ satisfying

- (i) $\delta(g) = \overline{g}$ for all $g \in H$,
- (ii) $\delta(g)^{-1}\overline{g}$ centralises \overline{kH} for all $g \in G$.

Then there exists an isomorphism of pseudocompact k -algebras

$$\Psi : \overline{kG} \rightarrow \overline{kH} \hat{\otimes}_k k[[G/H]],$$

where $\hat{\otimes}$ denotes the completed tensor product.

Proof. Firstly, the function $G \rightarrow \left(\overline{kH} \hat{\otimes}_k k[[G/H]] \right)^\times$ given by

$$g \mapsto \delta(g) \otimes gH$$

is clearly a continuous group homomorphism, and so the universal property of completed group rings allows us to extend this function uniquely to a continuous ring homomorphism

$$\Psi' : kG \rightarrow \overline{kH} \hat{\otimes}_k k[[G/H]].$$

In the same way, we may extend δ uniquely to a map $\delta : kG \rightarrow \overline{kH}$, and by assumption (i), $\delta|_{kH}$ is just the natural quotient map $kH \rightarrow \overline{kH}$. Hence $\ker \delta$ must contain the two-sided ideal IkG , so that Ψ' descends to a continuous ring homomorphism

$$\Psi : \overline{kG} \rightarrow \overline{kH} \hat{\otimes}_k k[[G/H]].$$

We claim that this is the desired isomorphism. To show that Ψ is an isomorphism, we will construct a continuous ring homomorphism

$$\Phi : \overline{kH} \hat{\otimes}_k k[[G/H]] \rightarrow \overline{kG}$$

and show that Φ and Ψ are mutually inverse.

Consider the continuous function $\varepsilon : G \rightarrow \overline{kG}^\times$ given by

$$\varepsilon(g) = \delta(g)^{-1} \overline{g}.$$

ε is a group homomorphism: indeed, for all $g, h \in G$, we have

$$\begin{aligned} \varepsilon(g)\varepsilon(h) &= \delta(g)^{-1} \overline{g} \delta(h)^{-1} \overline{h} \\ &= \boxed{\delta(g)^{-1} \overline{g}} \boxed{\delta(h)^{-1}} \overline{h} \\ &= \boxed{\delta(h)^{-1}} \boxed{\delta(g)^{-1} \overline{g}} \overline{h} && \text{by assumption (ii)} \\ &= \delta(gh)^{-1} \overline{gh} = \varepsilon(gh). \end{aligned}$$

It is clear that, by assumption (i), $\ker \varepsilon$ contains H , and so descends to a continuous group homomorphism $\varepsilon : G/H \rightarrow \overline{kG}^\times$; and so again by the universal property we get a continuous ring homomorphism $\varepsilon : k[[G/H]] \rightarrow \overline{kG}$. We also clearly have a continuous inclusion $\overline{kH} \rightarrow \overline{kG}$.

These functions, and the universal property of Definition 2.4, allow us to define the desired map $\Phi : \overline{kH} \hat{\otimes}_k k[[G/H]] \rightarrow \overline{kG}$ by

$$\Phi(x \otimes y) = x\varepsilon(y).$$

It now remains only to check that Φ and Ψ are mutually inverse. Indeed, for all $g \in G$ and $x \in \overline{kH}$,

$$\begin{aligned} \Phi(\Psi(\overline{g})) &= \Phi(\delta(g) \otimes gH) \\ &= \Phi(\delta(g) \otimes H) \Phi(1 \otimes gH) \\ &= (\delta(g))(\varepsilon(g)) \\ &= \overline{g}, \end{aligned}$$

and

$$\begin{aligned} \Psi(\Phi(x \otimes gH)) &= \Psi(x\varepsilon(g)) \\ &= \Psi(x\delta(g)^{-1}) \Psi(\overline{g}) \\ &= (x\delta(g)^{-1} \otimes 1)(\delta(g) \otimes gH) \\ &= x \otimes gH. \end{aligned}$$

□

Remark. Let M be a minimal prime of kG , and $e \in \overline{\text{cpi}^{k\Delta^+}}(M)$ (as in Notation 1.2). For most of the rest of this paper, we will insist on the mild condition that G centralise e , or equivalently that $M \cap k\Delta^+$ remain prime as an ideal of $k\Delta^+$. This is mostly to keep the notation simple: we will return briefly to this issue in section 6, and show that we have not lost much generality by doing this.

Corollary 2.6. Let G be a compact p -adic analytic group, k a finite field of characteristic p , and M a minimal prime of kG . In Notation 1.2, choose $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$, and assume (as in the above remark) that G centralises e , so that $(1 - e)\overline{kG} = \overline{M}$ and

$$kG/M \cong \overline{kG}/\overline{M} = e \cdot \overline{kG}.$$

Suppose we are given a continuous group homomorphism

$$\delta : G \rightarrow (e \cdot \overline{k\Delta^+})^\times,$$

satisfying

- (i) $\delta(g) = e \cdot \overline{g}$ for all $g \in \Delta^+$,
- (ii) $\delta(g)^{-1}\overline{g}$ centralises $e \cdot \overline{k\Delta^+}$ for all $g \in G$.

Then there exists an isomorphism

$$\Psi : e \cdot \overline{kG} \rightarrow e \cdot \overline{k\Delta^+} \otimes_k k[[G/\Delta^+]],$$

and hence also an isomorphism

$$\psi : e \cdot \overline{kG} \rightarrow M_t(k'[[G/\Delta^+]])$$

for some positive integer t and some finite field extension k'/k .

Proof. In Theorem 2.5, take $H = \Delta^+$, and take I to be the ideal of $k\Delta^+$ generated by $J(k\Delta^+)$ and $1 - a$, where $a \in k\Delta^+$ is any element whose image in $\overline{k\Delta^+}$ is e . This gives the isomorphism

$$\Psi : e \cdot \overline{kG} \rightarrow e \cdot \overline{k\Delta^+} \hat{\otimes}_k k[[G/\Delta^+]];$$

but now, as $e \cdot \overline{k\Delta^+}$ is finite-dimensional as a vector space over k , [4, Lemma 2.1(ii)] implies that the right hand side is equal to the ordinary tensor product

$$e \cdot \overline{k\Delta^+} \otimes_k k[[G/\Delta^+]].$$

Now the isomorphism ψ is given by composing Ψ with the isomorphism of Lemma 1.1(iii). \square

Remark. Note that, when $G \cong N \times \Delta^+$ as in [3, 10.1], δ is simply taken to be the composite of the natural map $N \times \Delta^+ \rightarrow \Delta^+$ given by projection onto the second factor and the inclusion map $\Delta^+ \hookrightarrow (e \cdot \overline{k\Delta^+})^\times$.

3 Almost faithful ideals

Throughout this section:

- G is a compact p -adic analytic group, and k is a finite field of characteristic p ,
- M is a minimal prime ideal of kG and $e \in \text{cpi}^{\overline{k\Delta^+}} M$, so that Notation 1.2 applies
- assume further that G centralises e , and that we have an untwisting map

$$\delta : G \rightarrow (e \cdot \overline{kG})^\times$$

satisfying the hypotheses of Corollary 2.6, and write

$$\psi : e \cdot \overline{kG} \rightarrow M_t(k'[[G/\Delta^+]])$$

for the corresponding isomorphism given by Corollary 2.6,

- write $q : kG \rightarrow e \cdot \overline{kG}$ for the natural quotient map.

(We leave it until section 4 to find such a δ for a certain large class of groups G .)

In this setting, we have the following one-to-one correspondences of ideals:

$$\left\{ \begin{array}{l} \text{ideals of} \\ kG \text{ which} \\ \text{contain } M \end{array} \right\} \begin{array}{c} \xleftrightarrow{\quad} \\ \xleftarrow{\quad q \quad} \end{array} \left\{ \begin{array}{l} \text{ideals of} \\ e \cdot \overline{kG} \end{array} \right\} \begin{array}{c} \xleftrightarrow{\quad} \\ \xleftarrow{\quad \psi \quad} \end{array} \left\{ \begin{array}{l} \text{ideals of} \\ M_t(k'[[G/\Delta^+]]) \end{array} \right\} \begin{array}{c} \xleftrightarrow{\text{Morita} \\ \text{equiv.}} \\ \xleftarrow{\quad} \end{array} \left\{ \begin{array}{l} \text{ideals of} \\ k'[[G/\Delta^+]] \end{array} \right\}.$$

Lemmas 1.5 and 1.6 may now be interpreted as demonstrating that the first and third correspondences in this diagram preserve some notion of control (as defined in Definition 1.3). The middle correspondence trivially preserves control, as ψ is an isomorphism. We remark also that all three correspondences preserve primality, the third by Lemma 1.7.

In this section, we show that some appropriate notion of almost-faithfulness (see Definition 1.4) is also preserved by these correspondences. That is, let P be any ideal of kG containing M . Then we have

$$\psi \circ q(P) = M_t(\mathfrak{p}),$$

where \mathfrak{p} is some ideal of $k'[[G/\Delta^+]]$. Recall the definition of $(-)^{\dagger}$ from Definition 1.4: we intend to show that the groups P^{\dagger} (a subgroup of G) and \mathfrak{p}^{\dagger} (a subgroup of G/Δ^+) are closely related.

We will abuse notation to identify the two rings

$$e \cdot \overline{k\Delta^+} \otimes_k k[[G/\Delta^+]] = e \cdot \overline{k\Delta^+} \otimes_{k'} k'[[G/\Delta^+]]$$

in the obvious way. Then, laying out the structure more explicitly, we have

$$\Psi(e \cdot \overline{P}) = e \cdot \overline{k\Delta^+} \otimes_{k'} \mathfrak{p}$$

in the notation of Corollary 2.6.

Suppose that $g\Delta^+ \in \mathfrak{p}^\dagger$ for some $g \in G$, i.e. $(g-1)\Delta^+ \in \mathfrak{p}$. Then

$$(1 \otimes g\Delta^+) - (1 \otimes \Delta^+) \in \Psi(e \cdot \overline{P}),$$

so

$$\Phi(1 \otimes g\Delta^+) - \Phi(1 \otimes \Delta^+) = \delta(g)^{-1}\overline{g} - e \in e \cdot \overline{P}.$$

This motivates the following definition:

Definition 3.1. Write

$$P_\delta^\dagger = \{g \in G \mid \delta(g)^{-1}\overline{g} - e \in e \cdot \overline{P}\},$$

so that P_δ^\dagger is the kernel of the composite map

$$G \xrightarrow{\varepsilon} (e \cdot \overline{kG})^\times \xrightarrow{\sim} (kG/M)^\times \twoheadrightarrow (kG/P)^\times,$$

where $\varepsilon : G \rightarrow (e \cdot \overline{kG})^\times$ is defined by $\varepsilon(g) = \delta(g)^{-1}\overline{g}$. (As we saw in the proof of Theorem 2.5, ε is a continuous group homomorphism.) Compare this with Definition 1.4.

Now, since $\varepsilon(g) = 1$ for all $g \in \Delta^+$, we have $\Delta^+ \leq P_\delta^\dagger$ for any ideal P . We say that P is δ -faithful if $P_\delta^\dagger = \Delta^+$ (and P is δ -unfaithful if P_δ^\dagger is infinite).

Lemma 3.2. The following are equivalent:

- (i) P is almost faithful (as an ideal of kG).
- (ii) P is δ -faithful.
- (iii) \mathfrak{p} is faithful (as an ideal of $k'[[G/\Delta^+]]$).

Proof.

(ii) \Leftrightarrow (iii) By the above calculation, we see that P is defined to be a δ -faithful ideal of kG precisely when \mathfrak{p} is a faithful ideal of $k'[[G/\Delta^+]]$.

(i) \Leftrightarrow (ii) Let $m = |\text{im}(\delta)|$. Note that $m < \infty$ as k is assumed to be a finite field. Then $\delta(g^m) = 1$ for all $g \in G$, so

$$\begin{aligned}
g^m \in P_\delta^\dagger &\Leftrightarrow \delta(g^m)\overline{g^m}^{-1} - e \in e \cdot \overline{P} \\
&\Leftrightarrow \overline{g^m}^{-1} - e \in e \cdot \overline{P} \\
&\Leftrightarrow e(\overline{g^m}^{-1} - 1) \in e \cdot \overline{P} \\
&\Leftrightarrow \overline{g^m}^{-1} - \overline{1} \in \overline{P} \\
&\Leftrightarrow g^{-m} - 1 \in P \\
&\Leftrightarrow g^{-m} \in P^\dagger \\
&\Leftrightarrow g^m \in P^\dagger,
\end{aligned}$$

so writing $(P^\dagger)^m := \langle g^m | g \in P^\dagger \rangle$, and likewise $(P_\delta^\dagger)^m$, we see that these two subgroups are equal.

Now, suppose P is almost faithful, and so in particular P^\dagger is torsion; then the subgroup $(P^\dagger)^m = (P_\delta^\dagger)^m$ is also torsion, and since g^m is torsion for any $g \in P_\delta^\dagger$, we have that g must also be torsion. So P_δ^\dagger is a torsion subgroup of G . Hence it must be finite: indeed, given any open normal uniform subgroup U of G , the kernel of the composite map $P_\delta^\dagger \hookrightarrow G \rightarrow G/U$ is a subgroup of $U \cap P_\delta^\dagger$, which is trivial as U is torsion-free [5, 4.5]. So P_δ^\dagger embeds into the finite group G/U , and as P_δ^\dagger is also normal in G by Definition 3.1, it is a finite orbital subgroup of G and hence must be a subgroup of Δ^+ , i.e. P is δ -faithful. The converse is similar. \square

In summary:

Corollary 3.3. Assume the hypotheses of Corollary 2.6. Let P be an ideal of kG containing M , and denote by $q : kG \rightarrow kG/M$ the natural quotient map. Write $\psi \circ q(P) = M_t(\mathfrak{p})$, where \mathfrak{p} is an ideal of $k'[[G/\Delta^+]]$. Then \mathfrak{p} is faithful if and only if P is almost faithful; and \mathfrak{p} is prime if and only if P is prime. \square

4 Untwisting when G is finite-by-(pro- p)

In this section, we introduce a group A_H for each closed subgroup H of G . By studying the structure of the group A_G in the case when G/Δ^+ is pro- p , we will find an untwisting map $\delta : G \rightarrow (e \cdot \overline{k\Delta^+})^\times$ satisfying the conditions of Corollary 2.6.

Let G be a compact p -adic analytic group, k a finite field of characteristic p , M a minimal prime of kG , and $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$, which we continue to suppose is centralised by G . Then $e \cdot \overline{k\Delta^+} \cong M_t(k')$, and in particular its automorphisms are all inner by the Skolem-Noether theorem [11, Tag 074P].

Note that both G and $(e \cdot \overline{k\Delta^+})^\times$ act on the ring $e \cdot \overline{k\Delta^+}$ by conjugation, and so we get group homomorphisms $G \rightarrow \text{Inn}(e \cdot \overline{k\Delta^+})$ and $(e \cdot \overline{k\Delta^+})^\times \rightarrow \text{Inn}(e \cdot \overline{k\Delta^+})$.

Definition 4.1. For any closed subgroup $H \leq G$, define A_H to be the fibre product of H and $(e \cdot \overline{k\Delta^+})^\times$ over $\text{Inn}(e \cdot \overline{k\Delta^+})$ with respect to the above maps,

$$A_H = (e \cdot \overline{k\Delta^+})^\times \times_{\text{Inn}(e \cdot \overline{k\Delta^+})} H,$$

a subgroup of $(e \cdot \overline{k\Delta^+})^\times \times H$. Write the projection map onto the second factor as $\pi_H : A_H \rightarrow H$.

As $e \cdot \overline{k\Delta^+} \cong M_t(k')$, we have $(e \cdot \overline{k\Delta^+})^\times \cong GL_t(k')$. The centre of $(e \cdot \overline{k\Delta^+})^\times$ is therefore isomorphic to $Z(GL_t(k'))$, which we will identify with k'^\times , and the inner automorphism group $\text{Inn}(e \cdot \overline{k\Delta^+})$ is isomorphic to $PGL_t(k')$. In particular, A_H is an extension of H by k'^\times . Indeed, the following diagram commutes and has exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & k'^\times & \xrightarrow{i} & A_H & \xrightarrow{\pi_H} & H \longrightarrow 1 \\ & & \parallel & & \downarrow & & \downarrow \\ 1 & \longrightarrow & k'^\times & \longrightarrow & (e \cdot \overline{k\Delta^+})^\times & \longrightarrow & \text{Inn}(e \cdot \overline{k\Delta^+}) \longrightarrow 1. \end{array}$$

The inclusion $i : k'^\times \rightarrow A_H$ is given by $i(x) = (x, 1)$. (The image of i is just $A_{\{1\}}$.)

We will now examine the subgroup structure of A_G .

Lemma 4.2. If N is a closed normal subgroup of G , then $A_N \triangleleft A_G$, and $A_G/A_N \cong G/N$.

Proof. Firstly, clearly A_N is naturally a subgroup of A_G , and the following diagram commutes and has exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & k'^\times & \longrightarrow & A_N & \xrightarrow{\pi_N} & N \longrightarrow 1 \\ & & \parallel & & \downarrow & & \downarrow \\ 1 & \longrightarrow & k'^\times & \longrightarrow & A_G & \xrightarrow{\pi_G} & G \longrightarrow 1. \end{array}$$

Let $(r, n) \in A_N$ and $(s, g) \in A_G$. For any $x \in (e \cdot \overline{k\Delta^+})$, we have $x^r = x^n$ and $x^s = x^g$, so we get $x^{s^{-1}rs} = x^{g^{-1}ng}$. As $g^{-1}ng \in N$, we have

$$(s, g)^{-1}(r, n)(s, g) = (s^{-1}rs, g^{-1}ng) \in A_N,$$

and so $A_N \triangleleft A_G$.

Hence we may take cokernels of the vertical maps, completing the above diagram to the following commutative diagram, whose columns and first two rows are exact:

$$\begin{array}{ccccccc}
& & 1 & & 1 & & 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & k'^{\times} & \longrightarrow & A_N & \longrightarrow & N \longrightarrow 1 \\
& & \parallel & & \downarrow & & \downarrow \\
1 & \longrightarrow & k'^{\times} & \longrightarrow & A_G & \longrightarrow & G \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & 1 & \longrightarrow & A_G/A_N & \longrightarrow & G/N \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 1 & & 1 & & 1
\end{array}$$

By the Nine Lemma, the third row is now also exact. \square

Consider the natural map $\Delta^+ \rightarrow (e \cdot \overline{k\Delta^+})^{\times}$ given by $g \mapsto e \cdot \overline{g}$. There is a “diagonal” inclusion map $d : \Delta^+ \rightarrow A_G$ given by $g \mapsto (e \cdot \overline{g}, g)$, and the image $d(\Delta^+)$ is normal in A_G : indeed, suppose we are given $(x, h) \in A_G$. Then

$$\begin{aligned}
d(g)^{(x, h)} &= (x, h)^{-1}(e \cdot \overline{g}, g)(x, h) \\
&= ((e \cdot \overline{g})^x, g^h) \\
&= ((e \cdot \overline{g})^h, g^h) && \text{by definition of } A_G \\
&= d(g^h).
\end{aligned}$$

Remark. The map d , considered as a map from Δ^+ to A_{Δ^+} , splits the map π_{Δ^+} .

Hence there are copies of k'^{\times} and Δ^+ in A_{Δ^+} , and they commute: given $x \in k'^{\times}$, $g \in \Delta^+$, we have

$$i(x)d(g) = (x, 1)(e \cdot \overline{g}, g) = (e \cdot \overline{g}, g)(x, 1) = d(g)i(x)$$

as x commutes with $e \cdot \overline{g}$ inside $e \cdot \overline{k\Delta^+}$. In other words,

$$A_{\Delta^+} = i(k'^{\times})d(\Delta^+) \cong k'^{\times} \times \Delta^+.$$

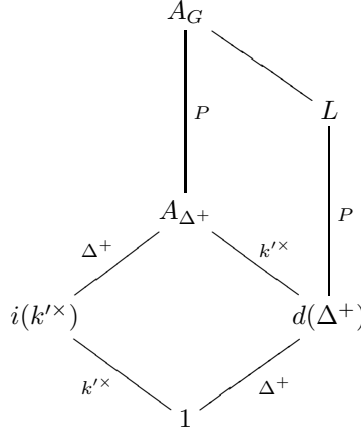
Lemma 4.3. Let G be a compact p -adic analytic group. Suppose that we have an injective group homomorphism $\sigma : G \rightarrow A_G$ splitting π_G such that, for all $g \in \Delta^+$, we have $\sigma(g) = (e \cdot \overline{g}, g)$. Then we can find a δ satisfying the conditions of Corollary 2.6.

Proof. Define δ to be the composite of $\sigma : G \rightarrow A_G$ with the projection $A_G \rightarrow (e \cdot \overline{k\Delta^+})^\times$. \square

We assume for the remainder of this section that G/Δ^+ is pro- p , and find a map σ satisfying Lemma 4.3 for this case.

Write $P = G/\Delta^+$. Note that $A_G/d(\Delta^+)$ is an extension of A_G/A_{Δ^+} (which is isomorphic to P , a pro- p group, by Lemma 4.2) by $A_{\Delta^+}/d(\Delta^+)$ (which is isomorphic to k'^\times , a p' -group, by the discussion above). Hence, as k is still assumed to be finite, we may apply Sylow's theorems [5, §1, exercise 11] to find a Sylow pro- p subgroup $L/d(\Delta^+)$ of $A_G/d(\Delta^+)$ which is isomorphic to P .

This information is summarised in the following diagram.



Lemma 4.4. Suppose G/Δ^+ is pro- p . Then there is a map σ splitting the surjection $\pi_G : A_G \rightarrow G$ satisfying the hypotheses of Lemma 4.3.

Proof. Consider $\pi_G|_L : L \rightarrow G$. Now, $\ker(\pi_G) = i(k'^\times)$, so

$$\begin{aligned} \ker(\pi_G|_L) &= i(k'^\times) \cap L \\ &= (i(k'^\times) \cap A_{\Delta^+}) \cap L \\ &= i(k'^\times) \cap (A_{\Delta^+} \cap L) \\ &= i(k'^\times) \cap d(\Delta^+) = 1, \end{aligned}$$

so $\pi_G|_L$ is injective. Also,

$$i(k'^\times) \cdot L = A_{\Delta^+} \cdot L = A_G,$$

so

$$\begin{aligned} G &= \pi_G(A_G) = \pi_G(i(k'^{\times}) \cdot L) \\ &= \pi_G(i(k'^{\times})) \cdot \pi_G(L) \\ &= \pi_G(L) \end{aligned}$$

as $\pi_G(i(x)) = \pi_G((x, 1)) = 1$ for $x \in k'^{\times}$, and hence $\pi_G|_L$ is surjective. So $\pi_G|_L$ is in fact an isomorphism $L \rightarrow G$.

Define $\sigma : G \rightarrow L \rightarrow A_G$ (i.e. $(\pi_G|_L)^{-1}$ followed by inclusion). By construction, this σ splits π_G . Also, as $\pi_G(\sigma(g)) = \pi_G(d(g)) = g$ for all $g \in \Delta^+$, we have that $\sigma(g)d(g)^{-1} \in \ker \pi_G \cap L = 1$, and so $\sigma(g) = d(g) = (e \cdot \bar{g}, g)$ for $g \in \Delta^+$ as required. \square

Now we may define $\delta : G \rightarrow (e \cdot \overline{k\Delta^+})^{\times}$ as in the proof of Lemma 4.3, allowing us to deduce the following theorem, in which we continue to write $q : kG \rightarrow e \cdot \overline{kG}$ for the natural quotient map:

Theorem 4.5. Let G be a compact p -adic analytic group with G/Δ^+ pro- p , and let k be a finite field. Write $N = G/\Delta^+$. Let M be a minimal prime of kG , and $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$, and suppose that e is centralised by G . Then we can find a $\delta : G \rightarrow (e \cdot \overline{k\Delta^+})^{\times}$ satisfying the conditions of Corollary 2.6. In particular:

- (i) There exists an isomorphism

$$\Psi : e \cdot \overline{kG} \rightarrow e \cdot \overline{k\Delta^+} \otimes_k kN.$$

- (ii) There exist a finite field extension k'/k and a positive integer t , and an isomorphism

$$\psi : e \cdot \overline{kG} \rightarrow M_t(k'N).$$

Furthermore, let A be an ideal of kG with $M \subseteq A$, so that $\psi \circ q(A) = M_t(\mathfrak{a})$ for some ideal \mathfrak{a} of $k'N$. Then:

- (iii) A is prime if and only if \mathfrak{a} is prime. Also, A is almost (G) -faithful if and only if \mathfrak{a} is (N) -faithful.

Proof.

- (i) The map δ as defined by Lemmas 4.3 and 4.4 satisfies the conditions of Corollary 2.6, which gives the isomorphism $\Psi : e \cdot \overline{kG} \rightarrow e \cdot \overline{k\Delta^+} \otimes_k k[[G/\Delta^+]]$.
- (ii) As in Corollary 2.6, we may identify $e \cdot \overline{k\Delta^+} \otimes_k k[[G/\Delta^+]]$ with $M_t(k'[[G/\Delta^+]])$ by appealing to Lemma 1.1(iii).
- (iii) This is just Corollary 3.3. \square

Proof of Theorem A. This is contained within the above theorem. \square

5 Central twists by 2-cocycles

First, some basic definitions.

Definition 5.1. Let A be a ring and G a group. Suppose we have a function *of sets*

$$\sigma : G \rightarrow \text{Aut}(A).$$

(We will write the image of $a \in A$ under the automorphism $\sigma(g)$ as $a^{\sigma(g)}$.) Let $\alpha : G \times G \rightarrow A$ be a function *of sets*.

If, for all $x, y, z \in G$, we have

$$\alpha(xy, z)\alpha(x, y)^{\sigma(z)} = \alpha(x, yz)\alpha(y, z), \quad (5.1)$$

then α is a *2-cocycle (with respect to σ)*. We will write the set of such functions α as

$$Z_\sigma^2(G, A).$$

Let G be a finite group, R a ring, and $S = R * G$ a fixed crossed product. Recall [9, §1] that this means that:

- S is a free R -module on a generating set $\overline{G} \subseteq S$, where $|\overline{G}| = |G|$, and we shall write its elements as \overline{g} for $g \in G$;
- multiplication in S is given by

$$\begin{aligned} r\overline{g} &= \overline{g}r^{\sigma(g)} && \text{for all } r \in R, g \in G, \\ \overline{g}h &= \overline{gh}\tau(g, h) && \text{for all } g, h \in G, \end{aligned}$$

where

$$\begin{aligned} \sigma : G &\rightarrow \text{Aut}(R), && \text{the action,} \\ \tau : G \times G &\rightarrow R^\times, && \text{the twisting,} \end{aligned}$$

are two functions *of sets* satisfying

$$\sigma(x)\sigma(y) = \sigma(xy)\eta(x, y) \quad (5.2)$$

$$\tau(xy, z)\tau(x, y)^{\sigma(z)} = \tau(x, yz)\tau(y, z), \quad (5.3)$$

where $\eta(x, y)$ is the automorphism of R given by conjugation by $\tau(x, y)$.

Equation (5.3) says that τ is a 2-cocycle for σ with values in R^\times .

Notation 5.2. We will often need to write this structure explicitly as

$$S = R \underset{\langle \sigma, \tau \rangle}{*} G.$$

Suppose we wish to define some new crossed product, keeping the action the same but changing the twisting, say

$$S' = R \underset{\langle \sigma, \tau' \rangle}{*} G.$$

For the rest of this section, until stated otherwise, we will write
 $A = Z(R^\times).$

Lemma 5.3. S' is a ring if and only if there exists $\alpha \in Z_\sigma^2(G, A)$ satisfying $\tau'(x, y) = \tau(x, y)\alpha(x, y)$ for all $x, y \in G$.

Proof. Equation (5.2), applied to both S and S' , gives

$$\begin{aligned} \sigma(x)\sigma(y) &= \sigma(xy)\eta(x, y) & \text{and} \\ \sigma(x)\sigma(y) &= \sigma(xy)\eta'(x, y) & \text{for all } x, y \in G, \end{aligned}$$

where $\eta(x, y)$ and $\eta'(x, y)$ are the automorphisms induced by conjugation by $\tau(x, y)$ and $\tau'(x, y)$ respectively. This implies that $\eta = \eta'$. In other words, writing $\alpha = \tau^{-1}\tau'$ pointwise, we see that conjugation by $\alpha(x, y)$ induces the trivial automorphism on R , and so

$$\alpha : G \times G \rightarrow Z(R^\times) = A,$$

and it follows from equation (5.3) that, in order for S' to be a ring, α must be a 2-cocycle for σ taking values in A . The converse is identical. \square

Definition 5.4. When the crossed product $S = R * G = R \underset{\langle \sigma, \tau \rangle}{*} G$ and the central 2-cocycle α are fixed, write the ring S' defined above as S_α : we will say that S_α is the *central 2-cocycle twist of S by α with respect to the decomposition $S = R \underset{\langle \sigma, \tau \rangle}{*} G$* , meaning that

$$S_\alpha = R \underset{\langle \sigma, \tau\alpha \rangle}{*} G.$$

Sometimes it will not be necessary to specify all of this information in full; we may simply refer to S_α as a *central 2-cocycle twist of S* , or similar.

Note that S_α depends not only on the map τ , but also on the choice of basis \overline{G} for $S = R * G$.

Remark. Fix a crossed product $S = R * G$, and choose some $\alpha \in Z_\sigma^2(G, A)$. Write the resulting crossed product decompositions as

$$S = \bigoplus_{g \in G} R\overline{g}, \quad S_\alpha = \bigoplus_{g \in G} R\hat{g}.$$

We say that S and S_α differ by a *diagonal change of basis* if, for each $g \in G$, there is some unit $u_g \in R^\times$ such that $\hat{g} = \bar{g}u_g$. (In particular, if S and S_α differ by a diagonal change of basis, they are isomorphic.) By [9, exercise 1.1], S and S_α differ by a diagonal change of basis if and only if α is a *2-coboundary* for σ , i.e. there is some function $\varphi : G \rightarrow R^\times$ with

$$\alpha(x, y) = \varphi(xy)^{-1} \varphi(x)^{\sigma(y)} \varphi(y)$$

for all $x, y \in G$. Hence S and S_α are non-isomorphic only if α has non-trivial cohomology class. But we will not develop this idea any further in this paper.

Remark. We note that similar twists have been studied by Aljadeff *et al.*, e.g. in [1].

Central 2-cocycle twists will occur naturally in the theory later. For now, we see where this will be applied:

Definition 5.5. [9, Lemma 12.3] Let R be a prime ring. An automorphism $\varphi : R \rightarrow R$ is *X-inner* if there exist nonzero elements $a, b, c, d \in R$ such that, for all $x \in R$,

$$axb = cx^\varphi d.$$

(Here x^φ denotes the image of x under φ .) Write $\text{Xinn}(R)$ to denote the subgroup of $\text{Aut}(R)$ of X-inner automorphisms.

Now let G be a group, and fix a crossed product

$$S = R * G = R \underset{\langle \sigma, \tau \rangle}{*} G.$$

Write $\text{Xinn}_S(R; G)$ for the normal subgroup of G consisting of elements $g \in G$ that act by X-inner automorphisms on R , i.e.

$$\text{Xinn}_S(R; G) = \sigma^{-1}(\sigma(G) \cap \text{Xinn}(R)).$$

Theorem 5.6. Fix a crossed product $S = R * G$ with R prime, G finite. Then $\text{Xinn}_S(R; G) = \text{Xinn}_{S_\alpha}(R; G)$ for every $\alpha \in Z_\sigma^2(G, A)$. In particular, if $\text{Xinn}_S(R; G) = 1$, then S_α is a prime ring for every $\alpha \in Z_\sigma^2(G, A)$.

Proof. It is clear from the definition that $\text{Xinn}_{S_\alpha}(R; G)$ depends only on the map σ , and so $\text{Xinn}_{S_\alpha}(R; G) = \text{Xinn}_S(R; G)$ for all α . A special case of [9, Corollary 12.6] implies that, if $\text{Xinn}_{S_\alpha}(R; G) = 1$, then S_α is a prime ring. \square

This theorem will be important in later work, but we will not return to it in this paper.

Now we turn our attention back to the problem of understanding quotients of completed group algebras.

Let G be a compact p -adic analytic group, M a minimal prime of kG , and $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$ centralised by G . In this more general case, we may not be able to find a group homomorphism

$$\delta : G \rightarrow (e \cdot \overline{k\Delta^+})^\times$$

satisfying the hypotheses of Corollary 2.6, so we may not be able to find an isomorphism

$$\psi : e \cdot \overline{kG} \rightarrow M_t(k'[[G/\Delta^+]]).$$

In this case, fix (by [5], [6]) an open normal pro- p (e.g. p -valued) subgroup N of G/Δ^+ , and write H for the preimage of N in G , so that by Theorem 4.5 we *do* get an isomorphism

$$\psi : e \cdot \overline{kH} \rightarrow M_t(k'N).$$

Now we will have to rely on the crossed product structure of kG . That is, writing $F = G/H$, we can find a crossed product decomposition

$$kG = kH * F.$$

In the following discussion, we will construct a related crossed product $k'N * F$ (not necessarily isomorphic to $k'[[G/\Delta^+]]$), and show that the isomorphism ψ extends to an isomorphism

$$\tilde{\psi} : e \cdot \overline{kG} \rightarrow M_t(k'N * F).$$

Studying the structure of this crossed product $k'N * F$ will allow us to understand the prime ideals of kG . In fact, we will show that $k'N * F$ is a central 2-cocycle twist of $k'[[G/\Delta^+]]$.

Recall the map $\delta : H \rightarrow (e \cdot \overline{k\Delta^+})^\times$ from Theorem 4.5, and continue to write

$$\begin{aligned} \varepsilon : H &\rightarrow (e \cdot \overline{kH})^\times \\ h &\mapsto \delta(h)^{-1} \overline{h} \end{aligned}$$

for all $h \in H$, as in the proof of Theorem 2.5).

For the remainder of this section, we fix an element $g \in G$.

Fix $M_g \in (e \cdot \overline{k\Delta^+})^\times$, an arbitrary lift of the image of g under the map $G \rightarrow \text{Inn}(e \cdot \overline{k\Delta^+})$, i.e. any element such that $x^g = x^{M_g}$ for all $x \in e \cdot \overline{k\Delta^+}$, and hence $(M_g, g) \in A_G$. Define

$$\tilde{g} = M_g^{-1} \overline{g} \in (e \cdot \overline{kG})^\times \tag{5.4}$$

– this element will play the role of “ $\varepsilon(g)$ ” when $g \notin H$.

Conjugation by \tilde{g} is a ring automorphism $\varphi_g \in \text{Aut}(e \cdot \overline{kH})$, which induces a ring automorphism

$$\Psi \circ \varphi_g \circ \Phi =: \theta_g \in \text{Aut}(e \cdot \overline{k\Delta^+} \otimes_k kN).$$

(For ease of notation, we will revert to writing these maps on the left.)

That is:

$$\begin{array}{ccc} e \cdot \overline{kH} & \xrightarrow{\varphi_g} & e \cdot \overline{kH} \\ \uparrow \Phi & & \downarrow \Psi \\ e \cdot \overline{k\Delta^+} \otimes_k kN & \xrightarrow{\theta_g} & e \cdot \overline{k\Delta^+} \otimes_k kN \end{array}$$

For ease of notation, we will write these maps on the left as before.

Given $r \in e \cdot \overline{k\Delta^+}$ and $h\Delta^+ \in N$, we wish to calculate $\theta_g(r \otimes h\Delta^+)$ explicitly.

We begin with a trivial remark:

Lemma 5.7. By construction, $\varphi_g(r) = r$, and so $\theta_g(r \otimes 1) = r \otimes 1$. \square

Next, a computational lemma:

Lemma 5.8. Suppose N is pro- p and k'^\times contains no non-trivial pro- p subgroups. Then $\delta(h)^g = \delta(h^g)$ for all $h \in H$.

Proof. Define $\beta_g : H \rightarrow (e \cdot \overline{k\Delta^+})^\times$ by $\beta_g(h) = \delta(h^g)^{-1} \delta(h)^g$. We aim to show that $\beta_g(h) = 1$ for all h .

For any $r \in e \cdot \overline{k\Delta^+}$, we have that

$$\begin{aligned} r^{\delta(h^g)} &= r^{h^g} \\ &= ((r^{g^{-1}})^h)^g \\ &= ((r^{g^{-1}})^{\delta(h)})^g = r^{\delta(h)^g}, \end{aligned}$$

and so $r^{\beta_g(h)} = r$, i.e. $\beta_g(h)$ is in the centre of $(e \cdot \overline{k\Delta^+})^\times$. So β_g is a map from H to k'^\times .

Let $h_1, h_2 \in H$. Since $\beta_g(h_1) = \delta(h_1^g)^{-1} \delta(h_1)^g$ is central in $(e \cdot \overline{k\Delta^+})^\times$, in particular it centralises $\delta(h_2^g)^{-1}$, and so

$$\begin{aligned} \beta_g(h_1 h_2) &= \delta((h_1 h_2)^g)^{-1} \delta(h_1 h_2)^g \\ &= \delta(h_2^g)^{-1} \delta(h_1^g)^{-1} \delta(h_1)^g \delta(h_2)^g \\ &= \boxed{\delta(h_2^g)^{-1}} \boxed{\delta(h_1^g)^{-1} \delta(h_1)^g} \delta(h_2)^g \\ &= \boxed{\delta(h_1^g)^{-1} \delta(h_1)^g} \boxed{\delta(h_2^g)^{-1}} \delta(h_2)^g \\ &= \beta_g(h_1) \beta_g(h_2), \end{aligned}$$

so β_g is a group homomorphism $H \rightarrow k'^\times$. Furthermore, when $h \in \Delta^+$,

$$\begin{aligned} \beta_g(h) &= \delta(h^g)^{-1} \delta(h)^g \\ &= (e \cdot \overline{h^g})^{-1} (e \cdot \overline{h})^g = 1. \end{aligned}$$

So $\Delta^+ \leq \ker \beta_g$, and so β_g in fact descends to a homomorphism from N (a pro- p group) to k'^\times (containing no non-trivial pro- p subgroups), and so must be trivial. \square

Continue to write $\varepsilon(h) = \delta(h)^{-1} \overline{h}$ for all $h \in H$. Then, finally, we can conclude:

Corollary 5.9. Suppose N is pro- p and k'^\times contains no non-trivial pro- p subgroups. Then $\varepsilon(h)^{\tilde{g}} = \varepsilon(h^g)$ for all $h \in H$.

Proof. We have

$$\begin{aligned} \varepsilon(h)^{\tilde{g}} &= \varepsilon(h)^g && \text{as } \varepsilon(h) \text{ centralises } M_g \\ &= (\delta(h)^g)^{-1} \overline{h^g} \\ &= (\delta(h^g))^{-1} \overline{h^g} && \text{by Lemma 5.8} \\ &= \varepsilon(h^g), \end{aligned}$$

as required. \square

Now we can calculate the action of θ_g on $e \cdot \overline{k\Delta^+} \otimes_k kN$:

Lemma 5.10. Given $r \in e \cdot \overline{k\Delta^+}$ and $h\Delta^+ \in N$, with N pro- p and k'^\times containing no non-trivial pro- p subgroups as above, we have

$$\theta_g(r \otimes h\Delta^+) = r \otimes (h\Delta^+)^{g\Delta^+}.$$

Proof.

$$\begin{aligned} \theta_g(r \otimes h\Delta^+) &= \Psi(\varphi_g(\Phi(r \otimes h\Delta^+))) \\ &= \Psi(\varphi_g(r\varepsilon(h))) && \text{by definition} \\ &= \Psi(r^{\tilde{g}}\varepsilon(h)^{\tilde{g}}) \\ &= \Psi(r\varepsilon(h^g)) && \text{by Corollary 5.9 and Lemma 5.7} \\ &= \Psi(\Phi(r \otimes h^g\Delta^+)) && \text{by definition} \\ &= r \otimes h^g\Delta^+ && \text{by Theorem 2.5} \\ &= r \otimes (h\Delta^+)^{g\Delta^+}. \end{aligned} \quad \square$$

Now finally we can prove the main theorem of this section.

Let G be a compact p -adic analytic group and H an open normal subgroup containing Δ^+ with H/Δ^+ a pro- p group. Suppose k is a finite field of characteristic p . Fix a minimal prime M of kH , and $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$, and suppose that e is centralised by G .

As H satisfies the conditions of Theorem 4.5, there exist a finite field extension k'/k and a positive integer t , and isomorphisms

$$\Psi : e \cdot \overline{kH} \rightarrow e \cdot \overline{k\Delta^+} \otimes_{k'} k'N,$$

$$\psi : e \cdot \overline{kH} \rightarrow M_t\left(k'[[H/\Delta^+]]\right).$$

(Note that, here, we have identified the two rings $e \cdot \overline{k\Delta^+} \otimes_k kN$ and $e \cdot \overline{k\Delta^+} \otimes_{k'} k'N$ as in Lemma 1.1(iii).)

Fix a crossed product decomposition

$$k'[[G/\Delta^+]] = k'[[H/\Delta^+]] \underset{\langle \sigma, \tau \rangle}{*} (G/H). \quad (\ddagger)$$

Theorem 5.11. Notation as above. Then there exists

$$\alpha \in Z_\sigma^2\left(G/H, Z(k'[[H/\Delta^+]]^\times)\right)$$

such that Ψ extends to an isomorphism

$$\tilde{\Psi} : e \cdot \overline{kG} \rightarrow e \cdot \overline{k\Delta^+} \otimes_{k'} (k'[[G/\Delta^+]])_\alpha,$$

where the 2-cocycle twist $(k'[[G/\Delta^+]])_\alpha$ is taken with respect to the crossed product decomposition (\ddagger) above, as defined in Definition 5.4.

Hence ψ also extends to an isomorphism

$$\tilde{\psi} : e \cdot \overline{kG} \rightarrow M_t\left((k'[[G/\Delta^+]])_\alpha\right).$$

Proof. We know that $e \cdot \overline{k\Delta^+} \cong M_t(k')$ for some t and k' by Lemma 1.1, and so $e \cdot \overline{k\Delta^+}$ contains a set $\{e_{ij}\}$ of t^2 matrix units. Set

$$Z_H := Z_{e \cdot \overline{kH}}(\{e_{ij}\}) \subseteq e \cdot \overline{kH},$$

the centraliser of all of these matrix units, and likewise $Z_G \subseteq e \cdot \overline{kG}$ and $Z_{\Delta^+} \subseteq e \cdot \overline{k\Delta^+}$. Then the statement and proof of [8, 6.1.5] show that

$$e \cdot \overline{kH} \cong e \cdot \overline{k\Delta^+} \underset{Z_{\Delta^+}}{\otimes} Z_H$$

and

$$e \cdot \overline{kG} \cong e \cdot \overline{k\Delta^+} \underset{Z_{\Delta^+}}{\otimes} Z_G.$$

Since $e \cdot \overline{k\Delta^+} \cong M_t(k')$, it is clear that $Z_{\Delta^+} \cong k'$, the diagonal copy of k' inside $M_t(k')$. Using the isomorphism Ψ of Theorem 4.5, we can also understand the structure of Z_H :

$$\Psi(Z_H) = Z_{\Delta^+} \underset{k}{\otimes} k[[H/\Delta^+]] \cong k'[[H/\Delta^+]],$$

so Ψ restricts to an explicit isomorphism $Z_H \rightarrow k'[[H/\Delta^+]]$. Now we would like to understand the structure of Z_G .

As $F := G/H$ is finite, we may write $\{x_1, \dots, x_n\}$ for a set of representatives in G of $F = \{x_1H, \dots, x_nH\}$.

For each x_i , form $\tilde{x}_i \in Z_G^\times$ as in equation (5.4). Then $e \cdot \overline{kG}$ is a free $e \cdot \overline{kH}$ -module of rank n : $e \cdot \overline{kG}$ can be written as the internal direct sum

$$e \cdot \overline{kG} = \bigoplus_{i=1}^n \tilde{x}_i (e \cdot \overline{kH}).$$

Intersecting both sides of this equation with Z_G gives

$$Z_G = \bigoplus_{i=1}^n \tilde{x}_i Z_H,$$

showing that Z_G is a crossed product $Z_H * F$, and is therefore isomorphic to $k'[[G/\Delta^+]] * F$. Lemma 5.10 may now be restated to say that this $k'[[H/\Delta^+]] * F$ is just a central 2-cocycle twist of $k'[[G/\Delta^+]]$. This is the map $\tilde{\Psi}$, and the map $\tilde{\psi}$ then also follows from Lemma 1.1(iii). \square

Further, keeping the above notation, let A be an ideal of kH with $M \subseteq A$. Continuing as before to write $q : kG \rightarrow e \cdot \overline{kG}$ for the natural quotient map, we see by Theorem 4.5 that $\psi \circ q(A) = M_t(\mathfrak{a})$ for some ideal \mathfrak{a} of $k'[[H/\Delta^+]]$.

Corollary 5.12. The following are equivalent:

- (i) A is G -stable as an ideal of kH .
- (ii) \mathfrak{a} is (G/Δ^+) -stable as an ideal of $k'[[G/\Delta^+]]$.
- (iii) \mathfrak{a} is (G/Δ^+) -stable as an ideal of $(k'[[G/\Delta^+]])_\alpha$.

Moreover, when these conditions hold, we have

$$\tilde{\psi} \circ q(AkG) = M_t\left(\mathfrak{a} \left(k'[[G/\Delta^+]]\right)_\alpha\right).$$

Proof. The equivalence of statements (ii) and (iii) is clear since, by definition, the conjugation action of G/Δ^+ on the ring $k'[[G/\Delta^+]]$ is the same as the conjugation action of G/Δ^+ on the ring $(k'[[G/\Delta^+]])_\alpha$. The equivalence of (i) and (ii) follows easily from Lemma 5.10. Then

$$\begin{aligned} \tilde{\psi} \circ q(AkG) &= (\tilde{\psi} \circ q(A)) \cdot (\tilde{\psi} \circ q(kG)) \\ &= M_t(\mathfrak{a}) \cdot M_t\left(\left(k'[[G/\Delta^+]]\right)_\alpha\right) \\ &= M_t\left(\mathfrak{a} \left(k'[[G/\Delta^+]]\right)_\alpha\right). \end{aligned} \quad \square$$

Proof of Theorem B. This follows from the above theorem. \square

Proof of Theorem C. Statement (ii) follows from the above corollary, while (i) and (iii) follow from Corollary 3.3. \square

6 Peirce decomposition

From section 2 onwards, we often stipulated a stronger condition than in Lemma 1.1, namely that the conjugation action of G on \overline{kG} should fix the idempotent e . In general, e will have some non-trivial (but finite) G -orbit, so it will only make sense to consider $f \cdot \overline{kG}$, where $f = e|_G$.

The following result already gives us a lot of information:

Lemma 6.1. [8, 6.1.6] Let R be a ring, and let $1 = e_1 + e_2 + \cdots + e_n$ be a decomposition of 1 into a sum of orthogonal idempotents. Let G be a subgroup of the group of units of R , and assume that G permutes the set $\{e_1, e_2, \dots, e_n\}$ transitively by conjugation. Then $R \cong M_n(S)$, where S is the ring $S = e_1 R e_1$. \square

For instance, if M is a faithful minimal prime of kG , $e \in \text{cpi}^{\overline{k\Delta^+}}(M)$ and $f = e|_G$, this lemma implies that

$$f \cdot \overline{kG} \cong M_n(e \cdot \overline{kG} \cdot e),$$

and it is easy to show that

$$e \cdot \overline{kG} \cdot e = e \cdot \overline{kG_1}$$

where G_1 is the closed subgroup of elements of G (here identified with the natural subgroup of $(f \cdot \overline{kG})^\times$) that fix e under conjugation.

Proof of Theorem D. This follows from Theorem B and Lemma 6.1. \square

Now, if P is any ideal containing M , and the image of $f \cdot \overline{P}$ in $M_n(e \cdot \overline{kG_1})$ is $M_n(e \cdot \overline{Q})$ for some ideal Q (with Q containing JkG , and \overline{Q} containing $1 - e$), it is easy to see that:

Lemma 6.2. P is prime if and only if Q is prime.

Proof. By Lemma 1.5, it suffices to show that $f \cdot \overline{P} \cong M_n(e \cdot \overline{Q})$ is prime if and only if $e \cdot \overline{Q}$ is prime; but this is true because Morita equivalence preserves primality (Lemma 1.7). \square

With a little more care, it is also possible to use the proof of Lemma 6.1 to show that

$$P^\dagger = \bigcap_{g \in G} (Q^\dagger)^g.$$

(See Lemmas 6.5 and 6.6 for a proof of this statement.)

In a future paper, we will show that certain prime ideals P of kG are controlled by certain closed normal subgroups H containing Δ^+ . By Lemma 1.5, it clearly suffices to show that

$$(f \cdot \overline{P} \cap f \cdot \overline{kH}) f \cdot \overline{kG} = f \cdot \overline{P}.$$

If now $f = e|_H$, we may apply Lemma 6.1 to reduce to the case when $f = e$, and then apply the isomorphism ψ of Theorem 5.11 and Lemma 1.6 to reduce the problem to a simpler one.

However, Lemma 6.1 is not always precise enough for our purposes. It may be the case that $f = e|_G \neq e|_H$, i.e. the G -orbit of e splits into more than one H -orbit: then $f \cdot \overline{kH}$ is not a full matrix ring, but a direct sum

$$f \cdot \overline{kH} = \left(f_H^{(1)} \cdot \overline{kH} \right) \oplus \cdots \oplus \left(f_H^{(s)} \cdot \overline{kH} \right)$$

of several matrix rings (which may be non-isomorphic), and the same tools become messier to apply.

For this reason, it will be useful to keep track of the isomorphism in Lemma 6.1 more carefully, and so we will develop a more precise set of tools for handling this isomorphism.

Let R be a ring, and fix a subgroup $G \leq R^\times$. Suppose we have a G -orbit of mutually orthogonal idempotents $e_1, \dots, e_r \in R$ whose sum is 1. Recall the *Pierce decomposition* of R with respect to this set of idempotents,

$$R = \bigoplus_{i,j=1}^r R_{ij} = \begin{pmatrix} R_{11} & R_{12} & \cdots & R_{1r} \\ R_{21} & R_{22} & \cdots & R_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ R_{r1} & R_{r2} & \cdots & R_{rr} \end{pmatrix},$$

where $R_{ij} := e_i R e_j$.

Remark. Each R_{ii} is naturally a ring with identity $1_{R_{ii}} = e_i$ under the multiplication inherited from R . Each R_{ij} is an (R_{ii}, R_{jj}) -bimodule, and the restriction of the multiplication map $R \otimes_R R \rightarrow R$ gives a homomorphism of (R_{ii}, R_{kk}) -bimodules $R_{ij} \otimes_{R_{jj}} R_{jk} \rightarrow R_{ik}$ for all i, j, k .

Let A be any ideal of R , and write $A_{ij} = A \cap R_{ij} = e_i A e_j$.

Lemma 6.3. $A_{ij} R_{kl} = \delta_{jk} A_{il}$ (where δ_{jk} is the Kronecker delta symbol).

Proof. If $j \neq k$, it is clear from the definitions that $A_{ij} R_{kl} = 0$.

Suppose $j = k$, and let $g \in G$ be such that $e_k g = g e_l$, so that $0 \neq e_k g e_l \in R_{kl}$. Then, given any $a \in A$, we can write

$$e_i a e_l = e_i a g^{-1} g e_l = (e_i a g^{-1} e_k)(e_k g e_l),$$

showing that $A_{il} \subseteq A_{ik} R_{kl}$. The reverse inclusion is trivial. \square

In this section, we aim to study the relationship between an ideal $A \triangleleft R$ and the various ideals $A_{ii} \triangleleft R_{ii}$. To that end, write for convenience $S_i := R_{ii}$ and $B_i := A_{ii}$ from now on. Also, we have fixed the group G inside R^\times : its analogue

inside S_i^\times is $e_i G e_i$, which we note is isomorphic to $G_i := \mathbf{C}_G(e_i)$ in the natural way.

Recall from Definition 1.4 that, if I is an ideal of kG , we define

$$I^\dagger = (I + 1) \cap G = \ker(G \rightarrow (kG/I)^\times).$$

Definition 6.4. With notation as above,

$$A^\dagger = (A + 1_R) \cap G = \ker(G \rightarrow (R/A)^\times),$$

$$B_i^\dagger = (B_i + 1_{S_i}) \cap G_i = \ker(G_i \rightarrow (S_i/B_i)^\times).$$

The following lemma relates these groups.

Lemma 6.5.

- (i) If $A \neq R$, then $A^\dagger \leq \bigcap_{i=1}^r G_i$.
- (ii) $A^\dagger = \bigcap_{i=1}^r B_i^\dagger$.
- (iii) The $\{B_i^\dagger\}$ are a G -orbit under conjugation.

Proof.

- (i) Suppose not: then there exist some $i \neq j$ and some $g \in A^\dagger$ with $e_i g = g e_j$, so that $e_i g e_i = 0$. Then

$$g - 1 \in A \implies e_i(g - 1)e_i \in A \implies e_i \in A,$$

but then by conjugating by elements of G we see that $e_k \in A$ for all k , and so $1 = \sum_k e_k \in A$, so $A = R$, which is a contradiction.

- (ii) $\boxed{\leq}$ Fix i . If $g - 1 \in A$, then $g \in G_i$ by the previous lemma, so $e_i(g - 1)e_i \in B_i$.

$\boxed{\geq}$ Let $g \in \bigcap_i B_i^\dagger$, so that $e_i g e_j = g e_i e_j = 0 \in A$ for all $i \neq j$, and $e_i(g - 1)e_i \in B_i \subseteq A$ for all i . Then $g - 1 = \sum_{i \neq j} e_i g e_j + \sum_i e_i(g - 1)e_i \in A$.

- (iii) A is G -stable, so if $e_i^g = e_j$ then $B_i^g = (e_i A e_i)^g = e_j A e_j = B_j$. Also, $G_i^g = G_j$. It follows that $(B_i^\dagger)^g = B_j^\dagger$. \square

We finish by applying this to the problem mentioned at the beginning of this section. Recall the definition of *control* from Definition 1.3.

Lemma 6.6. Let G be a compact p -adic analytic group, H a closed normal subgroup containing Δ^+ , and k a field of characteristic p . Let P be an ideal of kG containing a prime ideal.

Write $e \in \text{cpi}^{\overline{k\Delta^+}}(P)$, $f = e|_G$, where the G -orbit of $e = e_1$ is $\{e_1, \dots, e_r\}$. For each $1 \leq i \leq r$, write G_i for the stabiliser in G of e_i (so that $e_i \cdot \overline{kG} \cdot e_i = e_i \cdot \overline{kG_i}$),

and similarly $H_i = H \cap G_i$, and set Q_i equal to the preimage in kG_i of the ideal $e_i \cdot \overline{P} \cdot e_i \triangleleft e_i \cdot \overline{kG_i}$.

Then

- (i) P is controlled by H if and only if each Q_i is controlled by H_i ,
- (ii) $P^\dagger = \bigcap_{i=1}^r Q_i^\dagger$.

Proof. Take R to be $f \cdot \overline{kG}$, and identify G with its image in $(f \cdot \overline{kG})^\times$. Let A be the ideal $f \cdot \overline{P}$, and B_i the ideal $e_i \cdot \overline{Q_i}$.

Write $D = f \cdot \overline{kH}$ and $D_i = e_i \cdot \overline{kH_i}$. By Lemma 1.5, it suffices to show: $(A \cap D)R = A$ iff $(B_i \cap D_i)S_i = B_i$ for each i .

\Rightarrow Take the equation $(A \cap D)R = A$, and intersect it with S_i .

\Leftarrow Note that $\bigoplus_i B_i = \bigoplus_i (B_i \cap D_i)S_i$ by assumption, and we have automatically that $(A \cap D)R \subseteq A$. Since $\bigoplus_i S_i \subseteq R$, we have that

$$\bigoplus_i B_i = \bigoplus_i (B_i \cap D_i)S_i \subseteq (A \cap D)R \subseteq A.$$

Hence

$$\left(\bigoplus_i B_i \right) R \subseteq (A \cap D)R \subseteq AR = A,$$

i.e.

$$\left(\bigoplus_i A_{ii} \right) \left(\bigoplus_{j,k} R_{jk} \right) \subseteq (A \cap D)R \subseteq A.$$

But the left hand side can easily be computed by Lemma 6.3 and is equal to

$$\bigoplus_{i,k} A_{ik}$$

– that is, A .

This shows that P is controlled by H , completing the proof of (i).

Comparing Definitions 1.4 and 6.4, we can see that $P^\dagger = A^\dagger$ and $Q_i^\dagger = B_i^\dagger$. Statement (ii) is now a direct consequence of Lemma 6.5(ii). \square

Proof of Theorem E. This is the content of Lemma 6.6. \square

References

- [1] E. Aljadeff and D.J.S. Robinson. Semisimple algebras, Galois actions and group cohomology. *Journal of Pure and Applied Algebra*, 94:1–15, 1994.
- [2] K. Ardakov. Localisation at augmentation ideals in Iwasawa algebras. *Glasgow Mathematical Journal*, 48(2):251–267, 2006.
- [3] K. Ardakov and S.J. Wadsley. Characteristic elements for p -torsion Iwasawa modules. *J. Algebraic Geometry*, 15:339–377, 2006.
- [4] A. Brumer. Pseudocompact algebras, profinite groups and class formations. *Journal of Algebra*, 4:442–470, 1966.
- [5] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal. *Analytic Pro- p Groups*. Cambridge University Press, 1999.
- [6] Michel Lazard. Groupes analytiques p -adiques. *Publications Mathématiques de l’IHÉS*, 26:5–219, 1965.
- [7] J.C. McConnell and J.C. Robson. *Noncommutative Noetherian Rings*. American Mathematical Society, 2001.
- [8] Donald S. Passman. *Algebraic Structure of Group Rings*. John Wiley & Sons, 1977.
- [9] Donald S. Passman. *Infinite Crossed Products*. Academic Press Inc., 1989.
- [10] J.E. Roseblade. Prime ideals in group rings of polycyclic groups. *Proc. London Math. Soc.*, 36:385–447, 1978.
- [11] The Stacks Project Authors. *Stacks Project*. <http://stacks.math.columbia.edu>, 2016.
- [12] W. Woods. On the structure of virtually nilpotent compact p -adic analytic groups. Preprint, [arXiv:1608.03137](https://arxiv.org/abs/1608.03137) [math.GR], 2016.